ID: 679200
Sample Name: WLmNdxIHr3
Cookbook: default.jbs
Time: 11:57:09
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

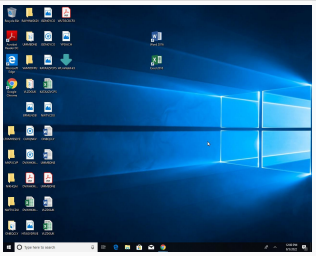
Windows Analysis Report

WLmNdxIHr3

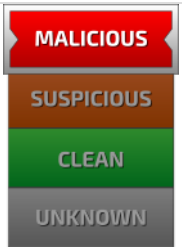
Overview

General Information

Sample Name:	WLmNdxIHr3 (renamed file extension from none to exe)
Analysis ID:	679200
MD5:	ba7863b67930a1..
SHA1:	0a90df33ba078b..
SHA256:	5cc3602f45772a...
Tags:	AgentTesla exe
Infos:	



Detection



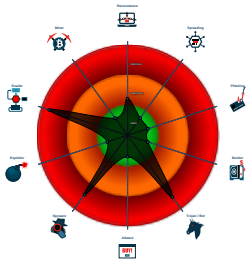
AgentTesla

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus / Scanner detection for sub...
- Tries to steal Mail credentials (via fi...
- Tries to harvest and steal Putty / W...
- Tries to harvest and steal ftp login c...
- .NET source code references suspic...
- Tries to detect sandboxes and other...
- Machine Learning detection for sam...
- Injects a PE file into a foreign proce...

Classification



Process Tree

- **System is w10x64**
- WLmNdxIHr3.exe (PID: 3360 cmdline: "C:\Users\user\Desktop\WLmNdxIHr3.exe" MD5: BA7863B67930A109864139EFE3DA478E)
  - WLmNdxIHr3.exe (PID: 3448 cmdline: C:\Users\user\Desktop\WLmNdxIHr3.exe MD5: BA7863B67930A109864139EFE3DA478E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "info@szlikestechs.com",
  "Password": "  Logistics@1234",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
WLmNdxIHr3.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.418888252.000000000356E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.425147984.0000000004E77000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.425147984.0000000004E77000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.425147984.0000000004E77000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x69f4e:$a13: get_DnsResolver • 0x9e56e:$a13: get_DnsResolver • 0xd298e:$a13: get_DnsResolver • 0x6873a:$a20: get_LastAccessed • 0x9cd5a:$a20: get_LastAccessed • 0xd117a:$a20: get_LastAccessed • 0x6a8cc:$a27: set_InternalServerPort • 0x9eeec:$a27: set_InternalServerPort • 0xd330c:$a27: set_InternalServerPort • 0x6abe5:$a30: set_GuidMasterKey • 0x9f205:$a30: set_GuidMasterKey • 0xd3625:$a30: set_GuidMasterKey • 0x68856:$a33: get_Clipboard • 0x9ce76:$a33: get_Clipboard • 0xd1296:$a33: get_Clipboard • 0x68864:$a34: get_Keyboard • 0x9ce84:$a34: get_Keyboard • 0xd12a4:$a34: get_Keyboard • 0x69b81:$a35: get_ShiftKeyDown • 0x9e1a1:$a35: get_ShiftKeyDown • 0xd25c1:$a35: get_ShiftKeyDown
00000004.00000000.408215753.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.WLmNdxIHr3.exe.4ee5310.9.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.WLmNdxIHr3.exe.4ee5310.9.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.WLmNdxIHr3.exe.4ee5310.9.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b11:$s10: logins • 0x66f31:$s10: logins • 0x32578:$s11: credential • 0x66998:$s11: credential • 0x2eb66:$g1: get_Clipboard • 0x62f86:$g1: get_Clipboard • 0x2eb74:$g2: get_Keyboard • 0x62f94:$g2: get_Keyboard • 0x2eb81:$g3: get_Password • 0x62fa1:$g3: get_Password • 0x2fe81:$g4: get_CtrlKeyDown • 0x642a1:$g4: get_CtrlKeyDown • 0x2fe91:$g5: get_ShiftKeyDown • 0x642b1:$g5: get_ShiftKeyDown • 0x2fea2:$g6: get_AltKeyDown • 0x642c2:$g6: get_AltKeyDown
0.2.WLmNdxIHr3.exe.4ee5310.9.raw.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x3025e:$a13: get_DnsResolver • 0x6467e:$a13: get_DnsResolver • 0x2ea4a:$a20: get_LastAccessed • 0x62e6a:$a20: get_LastAccessed • 0x30bdc:$a27: set_InternalServerPort • 0x64ffc:$a27: set_InternalServerPort • 0x30ef5:$a30: set_GuidMasterKey • 0x65315:$a30: set_GuidMasterKey • 0x2eb66:$a33: get_Clipboard • 0x62f86:$a33: get_Clipboard • 0x2eb74:$a34: get_Keyboard • 0x62f94:$a34: get_Keyboard • 0x2fe91:$a35: get_ShiftKeyDown • 0x642b1:$a35: get_ShiftKeyDown • 0x2fea2:$a36: get_AltKeyDown • 0x642c2:$a36: get_AltKeyDown • 0x2eb81:$a37: get_Password • 0x62fa1:$a37: get_Password • 0x2f62b:$a38: get_PasswordHash • 0x63a4b:$a38: get_PasswordHash • 0x3065e:$a39: get_DefaultCredentials
0.2.WLmNdxIHr3.exe.4ee5310.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 20 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

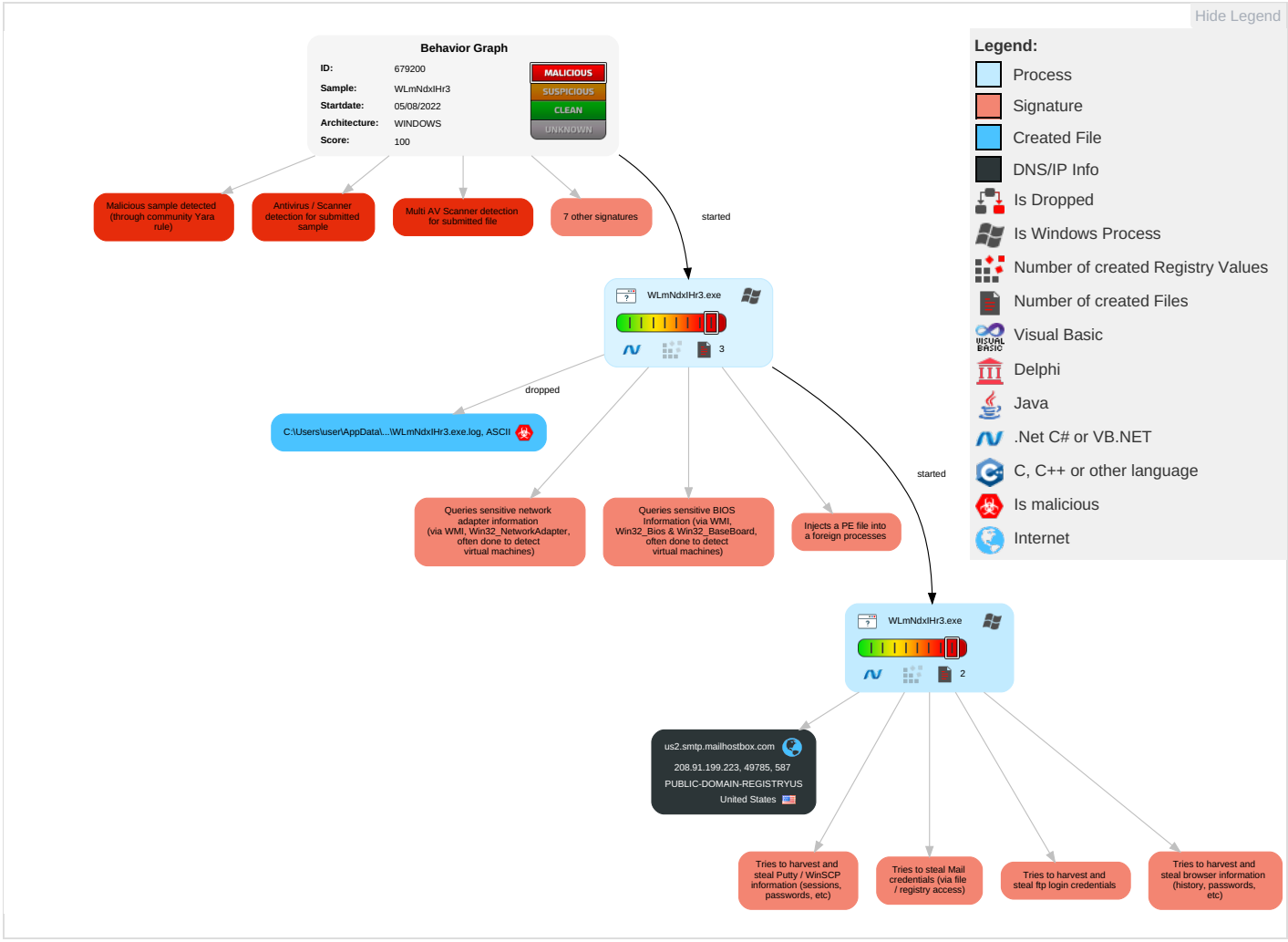
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
WLmNdxlHr3.exe	57%	Virustotal		Browse
WLmNdxlHr3.exe	34%	Metadefender		Browse
WLmNdxlHr3.exe	77%	ReversingLabs	Win32.Trojan.Leonem	
WLmNdxlHr3.exe	100%	Avira	TR/AD.AgentTesla.rlukc	
WLmNdxlHr3.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.WLmNdxlHr3.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://bladecoding.com/lolnotes/leagueofstats.php?name=	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://roTszh.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://JUpEVaHhlws.net	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high

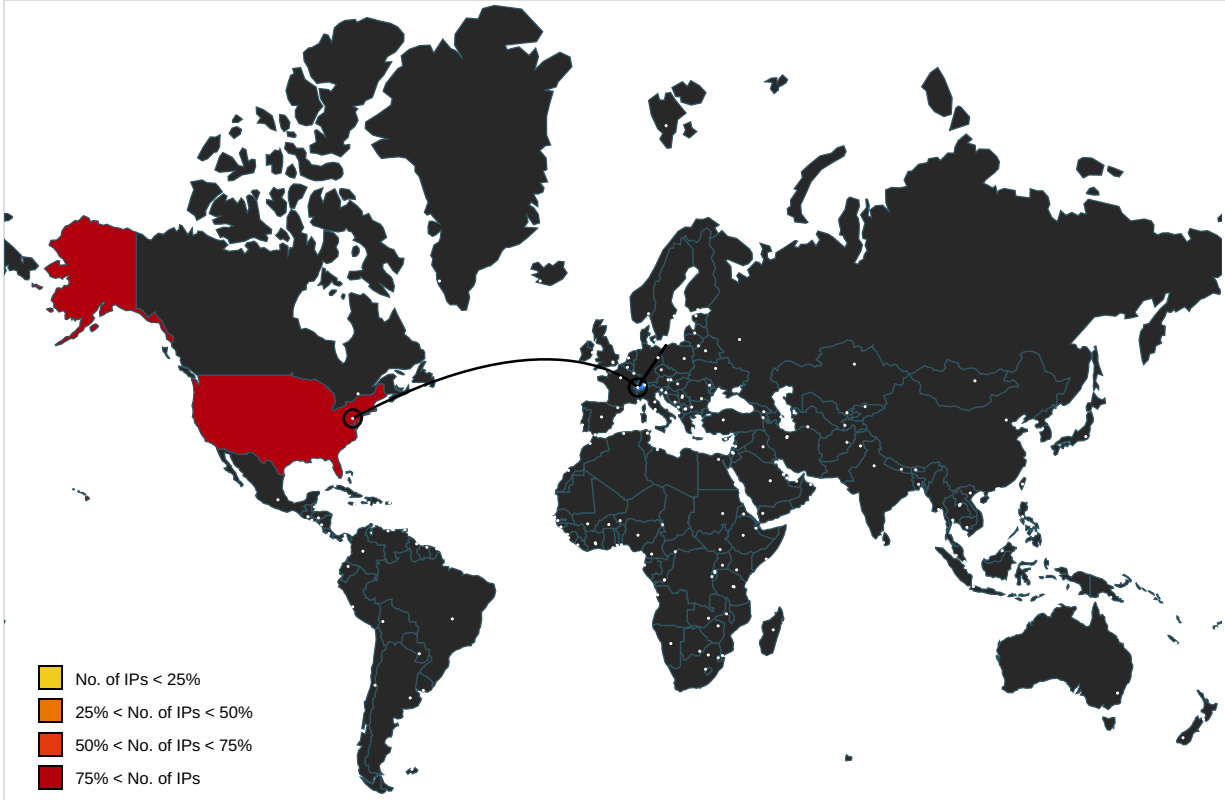
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	WLmNdxIHr3.exe, 00000004.00000002.640560502.0000000002F0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	WLmNdxIHr3.exe, 00000004.00000002.637950282.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://bladecoding.com/lolnotes/leagueofstats.php?name=	WLmNdxIHr3.exe	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	WLmNdxIHr3.exe, 00000004.00000002.640560502.0000000002F0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	WLmNdxIHr3.exe, 00000004.00000002.640560502.0000000002F0D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.lolking.net/summoner/	WLmNdxIHr3.exe	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	WLmNdxIHr3.exe, 00000004.00000002.637950282.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://bit.ly/unCoIY	WLmNdxIHr3.exe	false		high
http://www.tiro.com	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://raw.github.com/bladecoding/LoLNotes/master/General.txtO	WLmNdxIHr3.exe	false		high
http://www.fontbureau.com/designers	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/high6/LoLNotes	WLmNdxIHr3.exe	false		high
http://www.typography.netD	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://roTszh.com	WLmNdxIHr3.exe, 00000004.00000002.637950282.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	WLmNdxIHr3.exe, 00000004.00000002.637950282.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://JUpEVaHhlws.net	WLmNdxIHr3.exe, 00000004.00000002.640531921.0000000002F05000.00000004.00000800.00020000.00000000.sdmp, WLmNdxIHr3.exe, 00000004.00000002.637950282.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.sectigo.com0A	WLmNdxIHr3.exe, 00000004.00000002.640560502.0000000002F0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	WLmNdxIHr3.exe, 00000000.00000002.436103294.0000000007382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679200
Start date and time: 05/08/202211:57:09	2022-08-05 11:57:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WLmNdxIHr3 (renamed file extension from none to exe)
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.86
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:58:55	API Interceptor	657x Sleep call for process: WLmNdxIHr3.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WLmNdxIHr3.exe.log

Process:	C:\Users\user\Desktop\WLmNdxIHr3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.784555726017543
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	WLmNdxIHr3.exe
File size:	797696
MD5:	ba7863b67930a109864139efe3da478e
SHA1:	0a90df33ba078ba54576906d6072a11b8dca5356
SHA256:	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb
SHA512:	3cabfffd95d1151b04240caa2bf200c9a53cc3899f85927e3259f53805e2544dcdc4249b855bc4ffb245c1131d30ea48be52392928623ec1d0d4bb654212cc63
SSDEEP:	12288:zbv7n02b2UVFdPBGjy1AuFWBVeS5f/QBK7CNhvk0R4pRmCDqHVVAx67WeyqLvLqh:3Gjy1AuBS5c+Y7ipRmb13W4LzEkM
TLSH:	5105F12503BCCB4AE9BF47F9F4245581477AA203A54BE74D9F80E0CE3EA37A0D5152A7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*.b.....0..... .....(... ...@....@.. .....@.....

File Icon

Icon Hash:	686868e882e479b2

Static PE Info

General

Entrypoint:	0x4c28da
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62E02AA7 [Tue Jul 26 17:55:51 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
mov edi, edi
push ebp
mov ebp, esp
add byte ptr [eax], al
add byte ptr [ebp-75h], dl
in al, dx
pushad
mov eax, dword ptr [ebp+0Ch]
cmp word ptr [eax], 0002h
jne 00007FAAAD47EF24h
mov ecx, 00003308h
cmp word ptr [eax+02h], cx
jne 00007FAAAD47EF19h
mov dword ptr [eax+04h], 0100007Fh
popad
jmp 00007FAAAD47EF15h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2888	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x1ca4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc0910	0xc0a00	False	0.86008349894549	data	7.793379716498792	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x1ca4	0x1e00	False	0.65078125	data	6.816247600191881	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

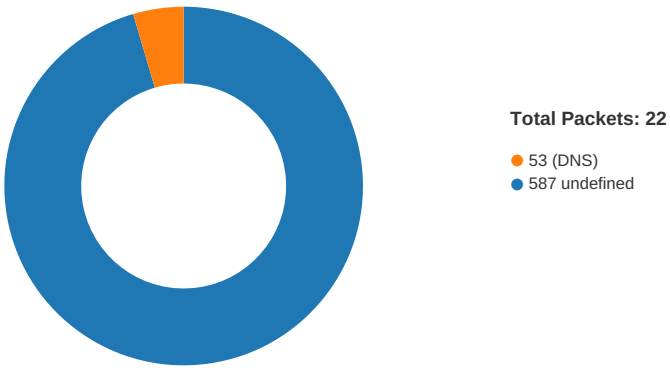
Name	RVA	Size	Type	Language	Country
RT_ICON	0xc4100	0xf94	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xc50a4	0x14	data		
RT_VERSION	0xc50c8	0x324	data		
RT_MANIFEST	0xc53fc	0x8a3	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:59:19.720238924 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:19.890372038 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:19.890538931 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:23.267518044 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.267951012 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:23.438301086 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.438460112 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.438792944 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:23.609215975 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.659852982 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:23.831017971 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.831059933 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.831079960 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.831099033 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.831321955 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:23.834280968 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:23.834434986 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:24.004659891 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:24.004803896 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:24.039912939 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:24.210659027 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:24.258789062 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:24.350205898 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:24.520832062 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:24.522891998 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:24.696552038 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:24.697578907 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:24.875669003 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:24.877111912 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:25.049618959 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.050239086 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:25.260646105 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.263529062 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.264116049 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:25.435524940 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.436611891 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.438678026 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:25.438939095 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:25.439802885 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:25.440084934 CEST	49785	587	192.168.2.7	208.91.199.223
Aug 5, 2022 11:59:25.609061003 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.610270977 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.748856068 CEST	587	49785	208.91.199.223	192.168.2.7
Aug 5, 2022 11:59:25.839360952 CEST	49785	587	192.168.2.7	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:59:19.661211014 CEST	64618	53	192.168.2.7	8.8.8.8
Aug 5, 2022 11:59:19.683432102 CEST	53	64618	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:59:19.661211014 CEST	192.168.2.7	8.8.8.8	0x9bdb	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

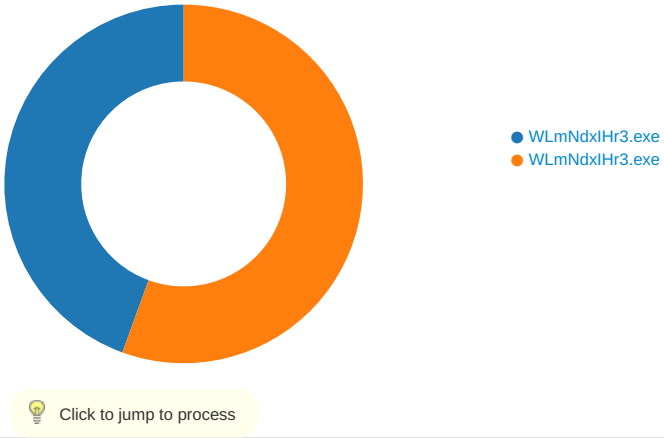
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 11:59:19.683432102 CEST	8.8.8.8	192.168.2.7	0x9bdb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Aug 5, 2022 11:59:19.683432102 CEST	8.8.8.8	192.168.2.7	0x9bdb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Aug 5, 2022 11:59:19.683432102 CEST	8.8.8.8	192.168.2.7	0x9bdb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Aug 5, 2022 11:59:19.683432102 CEST	8.8.8.8	192.168.2.7	0x9bdb	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 5, 2022 11:59:23.267518044 CEST	587	49785	208.91.199.223	192.168.2.7	220 us2.outbound.mailhostbox.com ESMTP Postfix
Aug 5, 2022 11:59:23.267951012 CEST	49785	587	192.168.2.7	208.91.199.223	EHLO 124406
Aug 5, 2022 11:59:23.438460112 CEST	587	49785	208.91.199.223	192.168.2.7	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Aug 5, 2022 11:59:23.438792944 CEST	49785	587	192.168.2.7	208.91.199.223	STARTTLS
Aug 5, 2022 11:59:23.609215975 CEST	587	49785	208.91.199.223	192.168.2.7	220 2.0.0 Ready to start TLS

Statistics

Behavior



System Behavior

Analysis Process: WLmNdxIHr3.exe PID: 3360, Parent PID: 4920

General

Target ID:	0
Start time:	11:58:39
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\WLmNdxIHr3.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\Desktop\WLmNdxIHr3.exe"
Imagebase:	0xde0000
File size:	797696 bytes
MD5 hash:	BA7863B67930A109864139EFE3DA478E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.418888252.000000000356E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.425147984.0000000004E77000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.425147984.0000000004E77000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.425147984.0000000004E77000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WLmNdxIHr3.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WLmNdxIHr3.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: WLmNdxIHr3.exe PID: **3448**, Parent PID: **3360**

General

Target ID:	4
Start time:	11:58:58
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\WLmNdxIHr3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\WLmNdxIHr3.exe
Imagebase:	0x830000
File size:	797696 bytes
MD5 hash:	BA7863B67930A109864139EFE3DA478E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.408215753.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.408215753.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000000.408215753.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.637950282.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.637950282.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\2c321486-cb67-48be-9b59-9780648ae894	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C001B4F	ReadFile

Disassembly

No disassembly